

A AL QAEDA E A INTERNET: O Perigo do “Planejamento Cibernético”

Tenente-Coronel (Res) Timothy L. Thomas, Exército dos EUA

PODEMOS afirmar, com bastante certeza, que a organização terrorista al Qaeda venera a Internet. Quando surgiu, a Internet foi celebrada como um meio integrador de culturas e um ambiente para permitir a comunicação ao comércio, consumidores e governos. Parecia oferecer oportunidades inigualáveis para a criação de uma comunidade global. Hoje, a Internet ainda oferece essa promessa, mas também provou, de certa forma, ser uma ameaça digital. O seu uso pelo grupo terrorista al Qaeda é apenas um exemplo disso. Tem também fornecido um campo de batalha virtual para hostilidades em tempos de paz entre Formosa e China, Israel e Palestina, Paquistão e Índia e a China e os EUA (durante a guerra em Kosovo e logo após a colisão entre as aeronaves *EP-3* da Marinha americana e o *MiG* chinês). Durante conflitos reais, a Internet foi usada como um campo de batalha virtual entre forças de coalizão da OTAN e elementos da população sérvia. Estas tensões reais dentre uma interface virtual envolveram não apenas nações-estados, mas também indivíduos e grupos não estatais, aliados a terceiros ou agindo individualmente.

Ampla evidência sugere que os terroristas usaram a Internet para planejar suas operações relativas aos ataques de 11 de setembro de 2001. Foi relatado que computadores confiscados no Afeganistão continham informação que revelou que a al Qaeda estava coletando inteligência sobre alvos e que enviava mensagens codificadas via a Internet. Em 16 de setembro de 2002, acredita-se que células da al Qaeda operando na América estavam usando serviços telefônicos via Internet para se comunicarem com outras células no além mar. Estes incidentes indicam que a Internet está sendo usada como uma ferramenta para “planejamentos cibernéticos” pelos terroristas. Ela prevê o anonimato aos terroristas assim como recursos de comando e controle e uma série de outras medidas para coordenar e integrar opções de ataque.

O planejamento cibernético pode de fato ser uma ferramenta mais importante para os terroristas do que a tão temida e infame opção do ciberterrorismo — ataques contra a informação e sistemas resultando em atos de violência contra alvos não combatentes. A Escola Naval de Pós-graduação (*Naval Postgraduate School — NPS*) definiu o ciberterrorismo como sendo a “destruição ou a interrupção ilegal de propriedade digital para intimidar ou coagir as pessoas”.¹ O planejamento cibernético, não definido pela *NPS* nem por outra fonte qualquer, refere-se à coordenação digital de um plano integrado, atravessando as fronteiras geográficas, que pode ou não resultar no derramamento de sangue. Pode incluir o ciberterrorismo como parte do plano geral. Desde 11 de setembro de 2001, fontes nos EUA têm monitorado vários *websites* com conexões à al Qaeda, que aparentam conter elementos de planejamento cibernético:

- *al Qaeda.com*, a qual oficiais dos EUA dizem ter contido informação codificada dirigindo membros da al Qaeda para outros sites mais seguros, oferecia notícias internacionais sobre a al Qaeda e publicava artigos, *fatwas* (decisões sobre a aplicação da lei muçulmana) e livros.
- *assam.com*, que se acreditava ser ligada à al Qaeda (o anfitrião originalmente era a *Scranton Company Burs-tNET Technologies, Inc.*), serviu como porta-voz da *jihad* no Afeganistão, na Chechênia e na Palestina.
- *almuhrajiroun.com*, um site da al Qaeda que urgia a simpatizantes assassinares o presidente paquistanês Musharraf.
- *qassam.net*, supostamente ligado ao *Hamas*.
- *jihadunspun.net*, que oferecia um vídeo de Osama bin Laden² de 36 minutos de duração.
- *7hj.7hj.com*, que tinha como finalidade ensinar a visitantes a como conduzirem ataques contra computadores.³
- *aloswa.org*, que publicava citações de gravações de

bin Laden, ordens religiosas que justificavam ataques terroristas e apoiavam a causa da al Qaeda.⁴

- drasat.com, dirigida pelo Centro de Pesquisas e Estudos Islâmicos (que alguns alegam ser um centro falso) e supostamente o mais crível dos sites islâmicos difundindo notícias da al Qaeda.

- jihad.net, alsaha.com e islammemo.com, supostamente haviam difundido declarações da al Qaeda nos seus sites.

- mvhoob.net e aljihad.online, supostamente difundiam canções político-religiosas com fotos de muçulmanos perseguidos, para criticar políticas americanas e líderes árabes, particularmente sauditas.⁵

Embora seja prudente monitorar as aplicações de planejamento cibernético via Internet que apóiam o terrorismo, deve ser compreendido que poucas (ou até mesmo nenhuma) delas são novas. Qualquer pirata eletrônico (*hacker*) ou mesmo um legítimo usuário da Internet pode empregar muitas destas mesmas medidas para uso próprio, negócios, ou até mesmo para fazer propaganda. A diferença, naturalmente, é que a maioria dos usuários da Internet, mesmo tendo o conhecimento para fazê-lo, não tem a mesma intenção de fazer o mal como tem o terrorista ou membro da al Qaeda.

Destacar várias das mais importantes aplicações pode ajudar a atrair a atenção às metodologias dos terroristas e permitir às agências de policiamento reconhecerem onde e o que devem procurar na Internet. Abaixo, listamos dezesseis medidas para considerar. Poderiam ser acrescentadas outras.

- *A Internet pode ser usada para determinar perfis.* A informação demográfica contida na Internet sobre os seus usuários permite aos terroristas identificarem aqueles que possam simpatizar com suas causas ou objetivos, solicitando-lhes doações, quando determinam ter encontrado um perfil apropriado. Geralmente, um grupo de fachada arrecadará os fundos para o terrorista, às vezes inocentemente. A arrecadação de fundos via correio eletrônico tem o potencial de significativamente apoiar os objetivos publicitários e financeiros do terrorista, simultaneamente.²

Uma busca de palavras-chave em jornais e diários *online* permite ao terrorista desenvolver um perfil dos meios criados para combater as suas próprias ações, ou um perfil das vulnerabilidades existentes em nossos sistemas. Por exemplo, artigos recentes publicaram notícias sobre tentativas de contrabandear itens por pontos de segurança ou controle. Uma tal publicação contava que, no aeroporto de Cincinnati, o contrabando conseguiu passar pela segurança 50 por cento das vezes. Uma simples busca na Internet, por um terrorista, revelaria essa falha, oferecendo a ele um ponto de partida para considerar em sua próxima operação. Um relatório do dia 16 de setembro observou que agências de policiamento nos

EUA estavam investigando chamadas feitas para células da al Qaeda no exterior, via cartões telefônicos, telefones celulares, cabinas de telefone ou serviços telefônicos na Internet. A exposição das técnicas de investigação dos órgãos de policiamento, permite ao terrorista alterar os seus próprios procedimentos operacionais. O uso, por parte do terrorista, da técnica de identificar perfis para descobrir tal material, presta grande apoio às suas operações de comando e controle. Isso implica em que, em uma sociedade livre como a dos EUA, pode-se publicar demasiada informação e, embora ela possa não ter tanto valor para nós, pode ser de grande utilidade para o terrorista.

- *O acesso à Internet pode ser controlado ou o seu uso dirigido de acordo com a configuração do servidor, criando assim uma arma verdadeiramente ideológica.* No passado, se um relatório era ofensivo a um governo, seu conteúdo podia ser filtrado ou censurado. Mas os governos não podem controlar a Internet da mesma forma que podem controlar os jornais ou as redes de televisão. De fato, a Internet pode servir ao terrorista como televisão, estação de rádio ou mesmo como um jornal internacional ou um diário. Ela permite a divulgação, em todo o mundo, de versões de eventos sem censura ou filtragem. Sites comunitários tais como os chat rooms (áreas de bate-papo), páginas pessoais e outros fóruns, existem praticamente sem censura ou com pouca filtragem de conteúdo. É um ambiente perfeito para um grupo com pouco financiamento explicar suas ações ou para amenizar críticas internas ou externas, especialmente quando usam servidores específicos. A Internet pode alcançar simples curiosos ou crentes fervorosos com diferentes mensagens, orientadas para a audiência-alvo.

Logo após os ataques do dia 11 de setembro de 2001, operadores da al Qaeda usaram a Internet para ganhar os corações e as mentes dos fiéis islâmicos em todo o mundo. Vários muçulmanos, internacionalmente reconhecidos e respeitados, que questionaram os ataques, foram descritos pela al Qaeda como sendo hipócritas. A al Qaeda manteve dois *websites* — *alned.com* e *drasat.com* — para discutir a “legalidade” dos ataques do dia 11 de setembro. Ela afirmou que o Islão não tem valores fundamentais em comum com o Ocidente e que os muçulmanos têm como finalidade espalhar o Islão pela espada. Como resultado de tal afirmação, vários muçulmanos, críticos da política da al Qaeda, retractaram a sua condenação inicial.⁷ A guerra ideológica funcionou.

- *A Internet pode ser usada de forma anônima, ou como um esconderijo para identidades.* Os terroristas têm acesso a ferramentas da Internet que lhes permite ficar anônimos ou disfarçar as suas identidades. Serviços de criptografia online oferecem chaves de criptografia para alguns serviços que são bem difíceis de decodificar. A página www.spammimic.com oferece ferramentas que

escondem texto codificado em mensagens de correio eletrônico não solicitadas (*spam*). A tecnologia de compressão de fala permite aos usuários converterem seus computadores em aparelhos telefônicos seguros. Contratos de acesso à Internet podem ser cancelados ou mudados sem maiores complicações. Por exemplo, usuários da Internet podem ter contratos de acesso com firmas como a *America Online — AOL*, e usar um programa de mensagens do tipo *AOL Instant Messenger*, a curto prazo. Além disso, o acesso anônimo é possível em muitas das milhares das áreas de bate-papo na Internet. Caso quiser, o usuário pode utilizar os cibercafés, computadores em universidades ou bibliotecas, ou outras fontes externas para esconder ainda mais a origem de suas mensagens.⁸ Um computador portátil (*laptop*) da al Qaeda, encontrado no Afeganistão, havia se conectado à Sociedade Anônima Francesa em várias ocasiões. Esse site oferece um Manual de Sabotagem em dois volumes online.

Não apenas existem métodos anônimos disponíveis para as pessoas que usam a Internet, como as vezes os próprios servidores da Internet participam, inocentemente, apoiando pessoas ou grupos com fins ilícitos. O site da al Qaeda foi originalmente encontrado na Internet na Malásia, até o dia 13 de maio. Reapareceu no Texas, em outro endereço, até o dia 13 de junho e de novo em Michigan, em 21 de junho. Foi finalmente fechado no dia 25 de junho de 2002. O servidor que hospedava a página aparentemente nada sabia a respeito do seu conteúdo, nem mesmo que a hospedava.⁹ Este jogo de esconde-esconde com sua página na Internet permitiu à al Qaeda permanecer funcionando apesar das várias tentativas de fechá-la. As campanhas de logro cibernéticas continuarão a ser um problema para as organizações policiais durante muitos anos.

- *A Internet produz um ambiente de medo virtual, ou de vida virtual.* É natural temer o que não se vê e o que não se compreende. A ameaça virtual de ataques cibernéticos parece ser uma dessas situações. O terror cibernético é gerado pelo fato de que aquilo que *poderia* acontecer em consequência de um ataque cibernético (o fechamento de companhias aéreas, a ruína de infra-estruturas críticas, desastres nas bolsas de valores, a divulgação de segredos do Pentágono, etc.) muitas vezes é associado com o que *acontecerá* de fato. As notícias nos levariam a crer que centenas ou milhares de pessoas continuam ativas na rede da al Qaeda só porque ela assim o afirma. Está claro que a Internet permite a pequenos grupos parecerem mais capazes do que são ou possam ser, tornando ameaças, às vezes vazias, em uma espécie de terror virtual. A Internet permite a terroristas amplificarem as consequências de suas ações com mensagens e ameaças dirigidas diretamente à população em geral, mesmo que o grupo esteja completamente impotente. Com efeito, a Internet permite a pessoas ou grupos parecerem ser maiores ou mais

importantes ou ameaçadores do que são na verdade.

A Internet pode ser usada para a desinformação e para o envio de mensagens aterradoras pessoais ou imagens assustadoras de atividades recentes (lembramos o uso da Internet para divulgar a morte do repórter Daniel Pearl por seus captores paquistaneses). Virtualmente, os ataques parecem ser bem planejados e controlados, as capacidades, genuínas. Mas as mensagens são geralmente unilaterais, refletindo uma política tendenciosa. Existe pouca oportunidade para verificar os fatos e descobrir se o que está sendo divulgado é real ou bravata. A Internet pode assim espalhar boatos e rumores que muitos, até investigarem mais a fundo, considerarão como sendo a verdade.

Recentemente, a estação de televisão Árabe, *al-Jazeera*, tocou gravações de discursos de Osama bin Laden e mostrou uma carta, supostamente assinada por ele, na qual mostrava sua satisfação com um ataque contra

A Internet é um excelente mecanismo de comando e controle. O comando e controle, do ponto de vista militar dos EUA, envolve o uso da autoridade e direção por parte de um comandante devidamente encarregado das forças designadas para o cumprimento da missão. Pessoal, equipamento, comunicações, repartições e procedimentos executam comando e controle por meio do apoio ao planejamento, à direção, à coordenação e ao controle das forças e das operações no cumprimento de uma missão.

um navio petroleiro perto do Iêmen e contra soldados americanos que participavam de um jogo de guerra no Kuwait. Estas mensagens foram coletadas e espalhadas pela Internet oferecendo prova virtual de que bin Laden continuava vivo. É mais provável que bin Laden tenha sido gravemente ferido (o que explicaria porque não se sabe nada dele há mais de um ano), mas a sua imagem pode ser manipulada via rádio ou pela Internet fazendo-o aparecer confiante e com boa saúde.

- *A Internet pode ajudar um grupo sem verba a arrecadar fundos.* A al Qaeda tem usado organizações de “caridade” humanitária islâmicas para arrecadar fundos para a *jihad* contra os que julgam ser inimigos do Islão. Analistas descobriram que a al Qaeda e certas agências de assistência humanitária têm usado as mesmas contas bancárias em várias ocasiões. O resultado tem sido que várias agências desse tipo, com sede nos EUA, foram fechadas por ordem das autoridades.¹⁰ O grupo extremista sunita *Hizb al-Tahrir* usa uma rede integrada de sites na

Internet na Europa e na África para divulgar um apelo para o retorno a um califado islâmico. Na rede, declaram desejar alcançar isso por meios pacíficos. Aqueles que os apóiam são incentivados a ajudar o esforço por meio de apoio financeiro, sábios pronunciamentos e encorajando outros a apoiarem a *jihad*. Informações bancárias, incluindo números de contas, eram fornecidas por um site na Alemanha, o www.explizit-islam.de.¹¹ Portais, especializados na transferência anônima de fundos, ou provendo serviços populares entre os terroristas (como a emissão de identidades ou passaportes oficiais), também encontram-se disponíveis.¹²

Os combatentes na república autônoma da Chechênia têm usado a Internet para divulgar os números de suas contas bancárias, para os quais os simpatizantes podem enviar contribuições. Uma dessas contas, de acordo com o site chechênio conhecido como amina.com, está em Sacramento, na Califórnia.

Naturalmente, existem outras maneiras de se obter dinheiro para uma causa usando a Internet. Uma das mais comuns é a fraude com cartões de crédito. Jean-Francois Ricard, um dos mais importantes investigadores de terrorismo da França, observou que muitos complôs terroristas islâmicos na Europa e no continente norte-americano foram financiados dessa maneira.¹³

• *A Internet é um excelente mecanismo de comando e controle.* O comando e controle, do ponto de vista militar dos EUA, envolve o uso da autoridade e direção por parte de um comandante devidamente encarregado das forças designadas para o cumprimento da missão. Pessoal, equipamento, comunicações, repartições e procedimentos executam comando e controle por meio do apoio ao planejamento, à direção, à coordenação e ao controle das forças e das operações no cumprimento de uma missão.

O comando e controle na Internet não sofre com as distâncias geográficas nem com a falta de equipamentos sofisticados de comunicações. Grupos antigovernamentais, presentes na conferência do G8 em Colônia, usaram a Internet para atacar computadores de centros financeiros e para coordenar protestos desde pontos tão distantes quanto a Indonésia e o Canadá. Terroristas podem usar suas organizações de fachada para a coordenação de tais ataques e para inundar o serviço de correio eletrônico de uma instituição importante (às vezes uma tática para despistar o verdadeiro ataque) ou mesmo para enviar mensagens codificadas para coordenar e planejar futuras operações.

Os cidadãos comuns, os que protestam contra o governo e os terroristas, agora têm acesso a meios de comando e controle, embora limitados, para coordenar e planejar ataques. Além disso, existem ferramentas disponíveis para detectar falhas nos sistemas de segurança e para procurar tirar proveito delas. Obter acesso a um site

permite ao infiltrado ou ao planejador comandar e controlar recursos (forças ou elétrons) de terceiros. O potencial da Internet para o comando e controle pode aumentar bastante a eficácia de uma organização que não tenha um comando e controle dedicado estabelecido, especialmente no que se refere à propaganda e à coordenação interna. Por último, o comando e controle pode ser executado via as salas de bate-papo da Internet. A al-Qaeda tem usado esse método, pelo site alned.com, para dispersar as suas forças para que operem independentemente, provendo-lhes liderança por meio da direção estratégica, de argumentos teológicos e de inspiração moral. Chegaram a publicar, na Internet, uma lista dos nomes e números de telefone de 84 combatentes da al Qaeda capturados no Paquistão, depois de terem escapado do Afeganistão. Presume-se que o motivo era para permitir que simpatizantes contatassem membros das famílias dos presos para lhes dizer que estes estavam vivos.¹⁴

• *A Internet é uma ferramenta de recrutamento.* A Internet permite ao usuário um controle completo sobre o conteúdo e elimina a necessidade de depender do jornalismo para a publicidade. Indivíduos simpatizantes de uma causa podem ser recrutados com imagens e mensagens de organizações terroristas. O surgimento dos vídeos digitais reforçou essa capacidade. As imagens e vídeos são ferramentas que dão poder aos terroristas e, de ainda mais importância, o acesso a tais produtos provê pontos de contato para homens e mulheres que queiram se unir à causa, seja ela qual for.¹⁵

*Versões atuais de programas de navegação (browsers) na Internet, incluindo o Netscape e o Internet Explorer, apóiam funções em JavaScript (linguagem criada pela Netscape que serve basicamente para aumentar os recursos do navegador). Isso permite aos servidores da Internet identificarem a linguagem definida do computador de um cliente em particular. Assim, o browser programado para usar o inglês como o idioma definido pode ser redirecionado para um site otimizado para publicidade dirigida a audiências ocidentais enquanto outro, definido em árabe, pode ser redirecionado para os sites estabelecidos para comunidades árabes ou muçulmanas.*¹⁶

Isto permite que o recrutamento seja feito no idioma da audiência desejada, utilizando a rede como alistadora de talentos específicos às causas terroristas. Recentemente, um site na Chechênia, que costumava apenas dirigir-se contra as forças russas operando na região, mudou o seu endereço na Internet para assam.com para incluir conexões à *jihad* no Afeganistão, na Palestina e na própria Chechênia. Tais sites dão a impressão que o mundo islâmico inteiro se está unindo contra o Ocidente quando, de fato, o mesmo pode ser o trabalho de apenas um punhado de indivíduos.

• *A Internet é usada para coletar informações sobre alvos em potencial.* O site operado pelo *Muslim Hackers*



Departamento de Defesa

O Sargento Philip Amiot do Destacamento de Vigilância de Longo Raio de Ação da 82ª Divisão Aeroterrestre usa um terminal remoto AN/PSC-5 Spitfire UHF e um computador laptop para enviar imagens aos satélites.

Club supostamente tinha conexão com sites nos EUA que afirmavam poder divulgar informações de caráter sigiloso, como codinomes e frequências de rádio usados pelo Serviço Secreto dos EUA. O mesmo site oferece aulas sobre a criação de vírus, estratégias para o acesso ilegal (*hacking*) a sites, redes e códigos secretos, assim como conexões a outros sites militantes islâmicos e “ciber-brincalhões” (*cyberpranksters*).¹⁷ Alvos recentes considerados pelos terroristas incluem os Centros de Controle e Prevenção de Doenças (*Centers for Disease Control and Prevention*) em Atlanta, o *FedWire*, sistema que supervisiona a movimentação de dinheiro, mantido pelo *Federal Reserve Board* e outras entidades que controlam o fluxo de informações na Internet.¹⁸ Ataques contra sistemas críticos de controle de infra-estruturas poderiam ser particularmente prejudiciais, especialmente contra sistemas do tipo do Sistema de Supervisão de Aquisição de Controle e Dados (*Supervisory Control and Data Acquisition — SCADA*). Qualquer informação sendo processada em redes sem a devida proteção dos protocolos de segurança pode resultar em danos potencialmente muito prejudiciais.

Os terroristas têm acesso, como muitos americanos, a dados contendo imagens de alvos em potencial, assim como a mapas, diagramas e outros dados cruciais sobre redes ou entidades importantes. Os dados de imagens

também podem permitir aos terroristas ver as atividades contraterroristas em um local-alvo. Um computador capturado da al Qaeda continha detalhes estruturais e de engenharia de uma represa, permitindo a engenheiros

A al Qaeda usa a polêmica na Internet não apenas para contrariar a reportagem ocidental mas também para contrapor-se a muçulmanos que não seguem a sua mesma convicção. Ela defende a sua guerra contra o Ocidente, incentiva a violência e se aproveita da Internet porque esta pode ser usada para enraivecer as pessoas e para neutralizar opiniões moderadas.

e planejadores da al Qaeda simularem danos e falhas catastróficas.¹⁹

Com relação à coleta de informações por meio da Internet, no dia 15 de janeiro de 2003, o Secretário de Defesa Donald Rumsfeld observou que um manual de adestramento da al Qaeda afirmava que “com o uso de recursos acessíveis ao público e sem ter que apelar para meios ilícitos, é possível coletar até 80 por cento das informações necessárias sobre o inimigo”.²⁰

- *A Internet distancia os que planejam o ataque dos seus alvos.* Terroristas planejando ataques contra os EUA podem fazê-lo de longe com pouco risco, especialmente se suas áreas de comando e controle estão localizadas em outros países. Traçar a rota de suas atividades é particularmente difícil. A Internet provê aos terroristas um local para planejamento sem os riscos normalmente associados com telefones celulares ou por satélites.

- *A Internet pode ser usada para roubar informação ou manipular dados.* Ronald Dick, Diretor do Centro Nacional para a Proteção da Infra-Estrutura (*National Infrastructure Protection Center*) do *FBI*, considera o roubo ou a manipulação de dados por parte de grupos terroristas como sendo o seu pior pesadelo, especialmente se os ataques são integrados com ataques físicos como, por exemplo, contra uma rede de energia nos EUA.²¹ Richard Clark, Chefe do Comitê de Proteção da Infra-Estrutura Crítica do Presidente (*President's Critical Infrastructure Protection Board*), diz que o problema da cibersegurança e da proteção de dados ficou claro com sua própria catástrofe no dia 18 de setembro de 2001, quando um vírus de codinome *Nimda* se espalhou pela Internet e, conseqüentemente, a computadores conectados à mesma em todo o mundo, causando bilhões de dólares em danos. O criador do vírus nunca foi identificado. O *Nimda*, praticamente ignorado por ter aparecido pouco depois dos ataques com as aeronaves e do susto com o antraz, iniciou uma reação em cadeia entre as companhias de software (incluindo a *Microsoft*) no sentido de levarem bem mais a sério as suas vulnerabilidades.²² No outono de 2001, um número de intrusões inexplicáveis começou a ocorrer nos computadores da *Silicon Valley* (região da Califórnia que concentra grande número de indústrias de manufatura e de alta tecnologia). Uma investigação por parte do *FBI* ligou as intrusões a equipamentos de telecomunicações na Arábia Saudita, na Indonésia e no Paquistão. Embora nenhum estivesse ligado diretamente à al Qaeda, há fortes suspeitas que o grupo esteve envolvido, de alguma forma.²³

- *A Internet pode ser usada para o envio de mensagens codificadas.* A prática da esteganografia — técnica de se esconder um arquivo dentro de outro, de forma criptografada — é uma arte muito usada pelos elementos criminosos e terroristas, em todo o mundo. Páginas escondidas, ou frases sem sentido aparente, podem ser ou conter instruções codificadas para agentes e simpatizantes da al Qaeda. Uma notícia recente reportou:

*A al Qaeda usa frases e símbolos codificados para dirigir os seus agentes. Um ícone de um AK-47 pode aparecer próximo a uma foto de Osama bin Laden, apontado um dia para um lado, e para o outro lado no dia seguinte. A cor dos ícones também pode mudar. As mensagens podem ficar escondidas em páginas dentro de sites sem conexões, ou colocadas abertamente em áreas de bate-papo.*²⁴

Fora isso, é possível comprar software de criptografia por menos de 15 dólares. Os ciberplanejadores obtêm vantagens quando escondem suas mensagens usando a criptografia. Às vezes, as mensagens nem sequer são escondidas de forma sofisticada. A televisão árabe *Al-Jazeera* reportou que a última mensagem de Mohammed Atta (outra vantagem da Internet: a impossibilidade de se verificar as fontes) dando as ordens para os ataques contra as Torres Gêmeas, foi simples e aberta. A mensagem supostamente dizia: “O semestre começa em mais três semanas. Temos 19 confirmações para estudo de direito, planejamento urbano, artes e engenharia.”²⁵ As referências feitas aos estudos aparentemente simbolizavam os edifícios que foram alvos dos ataques.

- *A Internet permite a grupos com poucos recursos sobrepujar até a enorme maquinaria de propaganda de países avançados.* Ela é um meio atraente para aqueles planejando um meio de atacar os grandes poderes por meio da mídia de massa. O fato da Internet estar sempre “ligada” permite a esses indivíduos não apenas acesso aos sites dia e noite, mas também lhes permite criticar os grandes poderes e tratá-los com desdém dentro de um foro público. A Internet pode ser usada para contrariar fatos e lógica com a lógica terrorista. Não há necessidade, por parte da organização terrorista, de se preocupar com a verdade já que, ignorar os fatos é procedimento operativo de praxe.

A al Qaeda usa a polêmica na Internet não apenas para contrariar a reportagem ocidental mas também para contrapor-se a muçulmanos que não seguem a sua mesma convicção. Ela defende a sua guerra contra o Ocidente, incentiva a violência e se aproveita da Internet porque esta pode ser usada para enraivecer as pessoas e para neutralizar opiniões moderadas. O site conhecido como o “Centro para o Estudo e Pesquisa do Islão” (supostamente um título dado às pressas), continha 11 seções e incluía reportagens sobre os combates no Afeganistão, a cobertura mundial do conflito na mídia, livros sobre a teologia da *jihad*, vídeos de testamentos de seqüestradores, informação sobre prisioneiros presos no Paquistão e na Baía de Guantanamo em Cuba e poesias *jihad*.²⁶

Não vale a pena uma grande potência mentir. Os fatos podem ser facilmente usados para contradizê-la. Até mesmo na guerra na Chechênia, houve momentos em que os chechenos afirmavam ter feito uma emboscada bem-sucedida contra um comboio russo e os russos o negavam terminantemente. Então, para provar o que tinha de fato ocorrido, os chechenos mostravam um vídeo da emboscada na Internet, contradizendo e ridicularizando a credibilidade da mídia russa oficial, minimizando o poder massivo da sua maquinaria propagandista. Oficiais da al Qaeda estão à espera para fazerem o mesmo com a mídia ocidental, se a oportunidade surgir.

- *A Internet pode ser usada para interferir com o comércio.* Esta tática exige o aproveitamento de oportu-

nidades precisas e o conhecimento detalhado do ambiente comercial do país alvo. Tenta prejudicar os negociantes, acusando-os de culpa por associação.

O *Hezbollah*, por exemplo, desenvolveu uma estratégia para desabilitar sites comerciais, militares e do governo de Israel com o objetivo de interromper as operações normais econômicas e da sociedade em geral. A primeira fase pode ser o bloqueio de sites oficiais do governo israelense; a segunda fase pode causar danos a sites financeiros — como os existentes na bolsa de valores de Israel; a terceira fase pode envolver ataques contra os principais servidores da Internet em Israel; e a quarta fase pode ser uma *blitz* contra sites comerciais israelenses na Internet para assegurar a perda de centenas de transações.²⁷ Uma fase final poderia ser acusar as companhias que negociam com o governo-alvo de culpadas por associação e apelar para o boicote dos produtos das mesmas. Terroristas árabes, por exemplo, atacaram a *Lucent Technologies* em uma série de ataques cibernéticos entre árabes e Israel.²⁸ Todos estes planos exigem conhecimentos detalhados que permitam o desenrolar das operações de forma precisa e em tempo oportuno.

- *A Internet pode mobilizar um grupo, exilados, ou outros hackers a agirem.* Os sites na Internet não são apenas usados para disseminar informações e propaganda. São também usados para criar solidariedade e irmandade entre grupos. No caso de organizações terroristas, a Internet compensa pela perda de bases e território. Nesse sentido, os sites mais importantes são a *alhed.com*, *jehad.net*, *drasat.com* e *aloswa.org* que citam, de Osama bin Laden, decretos religiosos que justificam ataques terroristas e que prestam apoio à causa da al Qaeda.²⁹ Além disso, operadores da Internet haviam estabelecido um site que era um “tipo de banco de dados ou uma enciclopédia para a disseminação de vírus de computadores”.³⁰ Esse site, o *7hj.7hj.com*, intencionava ensinar como conduzir ataques contra computadores, supostamente em nome do Islão.³¹

- *A Internet tira vantagem das normas legais.* Atores não estatais ou terroristas usando a Internet podem ignorar as noções legais ocidentais e focar, ao invés disso, em normas culturais ou religiosas. No mínimo, ignoram protocolos legais na própria Internet e usam a rede para violar as leis (acessando sites de maneira ilegal ou enviando vírus) enquanto, ironicamente, são protegidos por outras leis (escrutínio sem ordem judicial, etc).

Investigações internacionais dessas ações são difíceis de concluir devido aos mecanismos lentos de investigação de outras nações e o tempo limitado em que ficam guardados os dados.³² Porém, em consequência dos eventos de 11 de setembro de 2001 nos EUA, várias mudanças foram introduzidas no sistema legal americano para melhor combater os terroristas. Por exemplo, no passado, os assuntos relativos à privacidade dos usuários da Internet

eram de importância primária para o governo dos EUA. Depois de 11 de setembro, foi criada nova legislação.

A lei controversa *Patriot Act*, de 2001, incluiu nova orientação quanto ao crime contra a computação e à evidência eletrônica. A *Patriot Act* foi criada para unir e fortalecer os EUA, dando ao Governo as ferramentas apropriadas necessárias para interceptar e obstruir o terrorismo. Ela estabelece uma verba, no Departamento do Tesouro dos EUA, destinada a combater o terrorismo, cria emendas ao código penal federal autorizando processos de vigilância mais estritos, provê diretrizes para a investigação da lavagem de dinheiro, retira obstáculos à investigação

Os terroristas sabem que, quando aumentam o volume de suas mensagens e o seu uso das telecomunicações, os órgãos oficiais dos EUA emitem alertas. Dessa forma, os terroristas podem introduzir informações falsas em uma rede, de forma rotineira, analisar as respostas da comunidade de inteligência dos EUA e tentar desvendar as falhas e vulnerabilidades de seus próprios sistemas enquanto tentam determinar o tipo de tecnologia usada pelos EUA para descobrir os seus planos.

do terrorismo (dando autoridade ao *FBI* para investigar a fraude e atividades relacionadas a computadores em casos específicos), e reforça as leis criminais contra o terrorismo.³³

Um documento subsequente relaciona o poder das instituições do Governo com relação ao crime contra computadores e a evidência eletrônica, de acordo com a *Patriot Act*, provendo a autoridade para fazer várias coisas. Ele inclui: interceptar comunicações faladas durante investigações de acesso ilegal a computadores; permitir que agências de polícia rastreiem comunicações na Internet e em outras redes computadorizadas dentro do princípio “*pen register and trap and trace*” (que permite rastrear um sinal de volta à fonte); interceptar comunicações dos que acessam computadores ilegalmente; desenvolver e executar mandatos de busca de comunicações de correio eletrônico em toda a nação; e dissuadir e impedir o ciberterrorismo. Esta última provisão aumenta as penalidades máximas contra os *hackers* que causem danos a computadores protegidos (e elimina as penalidades mínimas); declara que os *hackers* precisam apenas mostrar a *intenção* de causar danos para serem formalmente acusados sem necessariamente causar os mesmos; prevê que seja levada em conta toda a extensão dos danos causados por ações do *hacker*; cria uma nova

ofensa relacionada a danos contra computadores usados para a segurança nacional e pela justiça; expande a definição de “computador protegido” para incluir computadores no estrangeiro; considera condenações anteriores, na esfera estadual, por crimes contra computadores, como ofensas anteriores; e define os danos ou perdas contra computadores. Além disso, o documento também desenvolve e apoia as capacidades forenses de cibersegurança.³⁴

• *A Internet pode ser usada para desviar a atenção de um ataque verdadeiro.* A al Qaeda pode enviar ameaças pela Internet ou via telefones celulares para desorientar agentes de segurança. Os terroristas estudam de que maneira os EUA coletam e analisam as informações e como respondem a elas.

Os terroristas sabem que, quando aumentam o volume de suas mensagens e o seu uso das telecomunicações, os órgãos oficiais dos EUA emitem alertas. Dessa forma, os terroristas podem introduzir informações falsas em uma rede, de forma rotineira, analisar as respostas da comunidade de inteligência dos EUA e tentar desvendar as falhas e vulnerabilidades de seus próprios sistemas enquanto tentam determinar o tipo de tecnologia usada pelos EUA para descobrir os seus planos. Por exemplo, se terroristas usam mensagens codificadas via telefone celular para discutirem uma operação falsa contra, digamos, a ponte *Golden Gate*, podem em seguida

ficar aguardando para ver se haverá reação por parte das agências de segurança com relação a essa famosa ponte em particular. Se detectarem reação, saberão que as suas comunicações estão sendo interceptadas por órgãos de segurança.³⁵

Concluindo, deve ser entendido que o ciberplanejamento é um conceito tão importante quanto o ciberterrorismo, talvez até mais. Os terroristas não encontrarão facilidade para interferir com a Internet. As vulnerabilidades são relatadas e consertadas continuamente enquanto os computadores funcionam sem muita interferência (pelo menos nos EUA). Espera-se que os agentes policiais e do governo façam maiores esforços contra as capacidades de ciberplanejamento dos terroristas para poder frustrar seus ataques contra computadores e outras atividades criminosas. No mínimo, a América pode usar tais medidas para tornar muito mais difícil para os terroristas coordenarem e controlarem as suas atividades. Paul Eedle, escrevendo no *The Guardian*, definiu o valor da Internet para a al Qaeda:

Já não importa para a organização se bin Laden ou o teórico egípcio Ayman al-Zawahiri e seus colegas estão em uma das montanhas do Hindu Kush ou vivem sem barba em algum subúrbio de Karachi. Podem inspirar e dirigir um movimento mundial sem estar em contato físico com os seus seguidores, sem saber quem eles são.

Tal é o poder e o perigo do ciberplanejamento. **MR**

Referências

1. Patricia Daukantas, "Government Computer News via Infowar.com," 14 de dezembro de 2001, <http://www.infowar.com>.
2. Jack Kelley, "Militants Wire Web with Links to Jihad," *USA Today*, 10 de julho de 2002, da *CNO/IO Newsletter*, 8-14 de julho de 2002.
3. *Ibid.*
4. Yossi Melman, "Virtual Soldiers in a Holy War," *Ha'aretz*, <http://www.haaretz.com>, 17 de setembro de 2002.
5. Habib Tabelesi, "Al-Qaeda Wages Cyber War against US," *Middle East Times*, Dubai, 27 de junho de 2002, rpt. na *CNO/IO Newsletter*, 1-7 de julho de 2002.
6. Patrick S. Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," documento não publicado, Escola de Estudos Militares Avançados (*School of Advanced Military Studies*), no Forte Leavenworth, Kansas, junho de 2002, p. 20.
7. Paul Eedle, "Al-Qaeda Takes Fight for 'Hearts and Minds' to the Web," *Jane's Intelligence Review*, agosto de 2002, na *CNO/IO Newsletter*, pp. 5-11 de agosto de 2002.
8. Tibbetts, pp 7, 9.
9. Eedle, "Al-Qaeda Takes Fight."
10. Colin Soloway, Rod Nordland, e Barbie Nadeau, "Hiding (and Seeking) Messages on the Web," na revista *Newsweek*, 17 de junho de 2002, p. 8.
11. "Sunni Extremist Group Hizb al-Tahrir Promotes Ideology on the Internet," FBIS, <http://199.221.15.211>, 5 de fevereiro de 2002.
12. C. E. Manin, "Terrorism and Information Communication Technology," *La Tribune*, College Interarmées de Defense, abril de 2002, p. 112.
13. Michael Elliot, "Reeling Them In," na revista *Time*, 23 de setembro de 2002, p. 33.
14. Paul Eedle, "Terrorism.com," *The Guardian*, 17 de julho de 2002, retirado do FBIS website no dia 17 de julho de 2002.
15. Tibbetts, p. 37.
16. *Ibid.*, p. 34.
17. Mark Hosenball, "Islamic Cyberterror," revista *Newsweek*, 20 de maio de 2002.
18. Tom Squitieri, "Cyberspace Full of Terror Targets," *USA Today*, 5 de junho de 2002.
19. Barton Gellman, "FBI Fears Al-Qaeda Cyber Attacks," *San Francisco Chronicle*, 28 de junho de 2002, pp. 1, 10.
20. "Citing Al Qaeda Manual, Rumsfeld Re-Emphasizes Web Security," *InsideDefense.com*, <http://www.insidedefense.com/>, 15 de janeiro de 2003.
21. Gellman, pp. 1, 10.
22. John Schwartz, "Despite 9/11 Warnings, Cyberspace Still at Risk," *The Post Standard* (Syracuse, N.Y.), 11 de setembro de 2002, pp. D-10, 11.
23. Maria T. Welch, "Accumulating Digital Evidence is Difficult," *The Post Standard*, 11 de setembro de 2002, pp. D-9, 11.
24. *Ibid.*; também Soloway, Nordland, e Nadeau.
25. Melman.
26. Eedle, "Terrorism.com."
27. Giles Trendle, "Cyberwars: The Coming Arab E-Jihad," *The Middle East*, No. 322 (abril de 2002), p. 6.
28. Tim McDonald, "Fanatics with Laptops: The Coming Cyber War," *NewsFactor.com* via *Yahoo! News*, 16 de maio de 2002.
29. Melman.
30. *Ibid.*
31. *Ibid.*
32. Manin, p. 112.
33. Veja "Bill Summary & Status for the 107th Congress," <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:@@L&summ2=m&>.
34. Veja "Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001," <http://www.cybercrime.gov/PatriotAct.htm>.
35. John Diamond, "Al-Qaeda Steers Clear of NSA's Ears," *USA Today*, 17 de outubro de 2002, *CNO/IO Newsletter*, 23-30 de outubro de 2002, pp. 17-18.
36. Eedle, "Terrorism.com."

O Tenente-Coronel (Res) Timothy L. Thomas é analista no Escritório de Estudos Militares Estrangeiros no Forte Leavenworth, Kansas. Escreveu extensivamente sobre operações de informações, combate urbano e operações de manutenção de paz, entre outros assuntos, incluindo quatro artigos prévios para a revista Parameters. Durante sua carreira militar, ele serviu na 82ª Divisão Para-quedista e foi o Chefe do Departamento de Assuntos Político- Militares Soviéticos no Instituto Russo do Exército dos EUA em Garmisch, na Alemanha.